PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-282991
(43)Date of publication of application : 15.10.1999

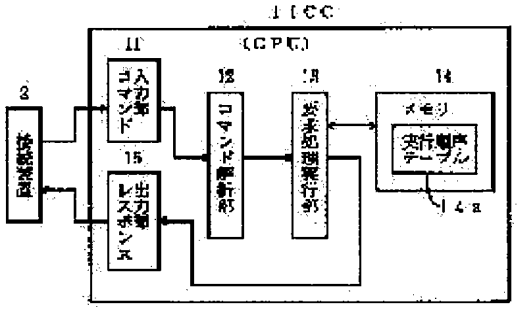
(51)Int.Cl. G06K 19/07
G06F 3/08
G06K 17/00
G06K 19/073

(21)Application number : 10-083468
(22)Date of filing : 30.03.1998

(71)Applicant : DAINIPPON PRINTING CO LTD
(72)Inventor : MORIYAMA AKIKO

(54) IC CARD

(57)Abstract:
PROBLEM TO BE SOLVED: To process a command as an error unless it is transmitted in previously decided order and to prevent illegal usage by providing a table where instruction executing order is registered in a non-volatile memory.
SOLUTION: An IC card(ICC) 1 is provided with an execution order table 14a for defining the execution order of commands in a memory 14. Each command for supporting ICC 1 has a unique command number, the execution order is registered in the table 14a by using the command number, the command which agrees with the registered execution order is properly processed and the command which does not agree is adopted as the error. When ICC 1 supports the three commands, that is, a reading command, a writing command and an erasing command, for example, the command numbers 01-03 are respectively assigned and, moreover, 04 is assigned to an authenticating command. The order is previously registered in the table 14a by using the command numbers.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－282991

(43)公開日　平成11年(1999)10月15日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｋ　19/07		Ｇ０６Ｋ　19/00	Ｎ
Ｇ０６Ｆ　3/08		Ｇ０６Ｆ　3/08	Ｃ
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｂ
			Ｅ
19/073		19/00	Ｐ

審査請求　未請求　請求項の数３　ＯＬ　（全 5 頁）

(21)出願番号　特願平10－83468

(22)出願日　平成10年(1998)３月30日

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号

(72)発明者　森山明子
東京都新宿区市谷加賀町一丁目１番１号大日本印刷株式会社内

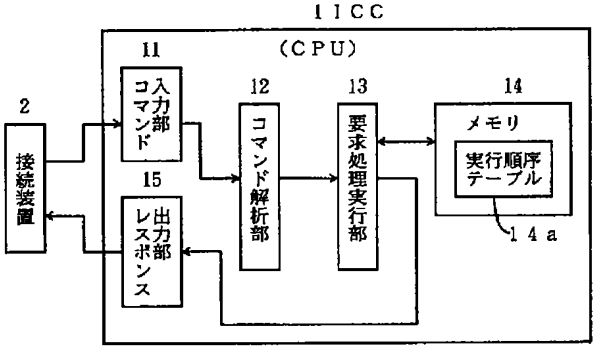
(74)代理人　弁理士　蛭川　昌信　（外７名）

(54)【発明の名称】　ＩＣカード

(57)【要約】

【課題】　予め定められた順序でコマンドが送信されない場合はエラーにして不正な使用を防ぐ。

【解決手段】　命令入力部１１、応答出力部１５、命令解析部１２、命令処理実行部１３、データを記憶する不揮発性メモリ１４を備えたＩＣカードにおいて、不揮発性メモリ１４に命令の実行順序を登録したテーブル１４ａを備えたものである。



1

【特許請求の範囲】
【請求項１】　命令入力部、応答出力部、命令解析部、命令処理実行部、データを記憶する不揮発性メモリを備えたＩＣカードにおいて、
不揮発性メモリに命令の実行順序を登録したテーブルを備えたことを特徴とするＩＣカード。
【請求項２】　請求項１記載のＩＣカードにおいて、各命令が実行順序を示す番号を備えたことを特徴とするＩＣカード。
【請求項３】　請求項１記載のＩＣカードにおいて、認証が成立したことを条件に、前記テーブルに規定された実行順序を書き換えることができる専用の命令を有することを特徴とするＩＣカード。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はＩＣカード（ＩＣＣ）に関する。
【０００２】
【従来の技術】近年、クレジットカードやプリペイドカード等さまざまな形でＩＣＣが使用され、ＣＰＵを内蔵して利便性の観点からいろいろな機能が付加されて汎用性を持たせたものが開発されている。このような従来のＩＣＣについてその概略を説明する。図８において、ＣＰＵを内蔵したＩＣＣ１は、接続装置２（インターフェース・デバイス：ＩＦＤ）からの処理要求であるコマンド（命令）を受け付けるコマンド入力部１１、受け付けたコマンドを解析するコマンド解析部１２、解析したコマンドに基づき要求されている処理を実行する要求処理実行部１３、処理の実行過程においてアクセスされるメモリ１４、処理結果をレスポンスとして接続装置２へ返すレスポンス出力部とからなっている。
【０００３】接続装置２とＩＣＣ１の間で交換される情報（コマンド、レスポンス）の最小単位はキャラクタであり、図９に示すように、先頭からスタートビット（ＳＴ）、８個のデータビット（ａ～ｈ）・パリティビット（ｉ）の順に送信され、直後にキャラクタ保護時間（ＧＴ）が１ビット以上続く形になっている。
【０００４】このようなキャラクタ複数個から、例えばＴ＝１ブロック伝送プロトコルを利用する場合、図１０に示すような情報ブロックが構成される。情報ブロックは、先頭フィールド、情報フィールド（ＩＮＦ）、最終フィールドからなり、先頭フィールドは、ブロックの送信元のアドレス、あて先アドレス及びＶＰＰ端子の状態制御を示すノードアドレス（ＮＡＤ）１バイト、伝送制御情報を含むプロトコル制御バイト（ＰＣＢ）１バイト、および情報フィールド長（ＬＥＮ）１バイトからなり、情報フィールドは、最大２５４バイトまで挿入可能であり、ブロックの最後は必ず誤り検出符合（ＥＤＣ）１または２バイトとなる。なお、各１バイトには、実際にはＳＴビット、パリティ検査ビット、ＧＴが付加されている。

2

【０００５】接続装置２からＩＣＣ１に送られるコマンドは図１０に示すブロックの情報フィールド内に収められ、図１１に示すように、見出し部と本体部から構成される。見出し部は、ＩＳＯのコマンドか否かを示すクラスバイト（ＣＬＡ）、命令コード（ＩＮＳ）、アクセスするファイルを指示するパラメータＰ１、Ｐ２からなり、本体部はコマンドデータフィールドバイト長（Ｌｃ）、コマンドデータフィールド（ｃデータ：可変長）、レスポンスデータフィールド長（Ｌｅ）からなっている。
【０００６】また、ＩＣＣ１から接続装置２へ送られるレスポンスは、図１２に示すように、本体部、後続部からなり、先頭からレスポンスデータフィールド（ｒデータ）、処理結果を示すステータスデータバイト１（ＳＷ１）、ステータスデータバイト２（ＳＷ２）の順に送られる。
【０００７】
【発明が解決しようとする課題】ところで、ＩＣＣではその内部で実行するコマンドのシーケンス（順序）に関してほとんどチェック機能を持たず、外部システム（接続装置）側での管理に任されていた。しかし、近年では偽造ＩＣカードや偽造端末による不正を防ぐためにＩＣカード利用シーケンスを監視する機能がＩＣカード側にも必要になってきた。
【０００８】本発明は上記課題を解決するためのもので、ＩＣカード内にチェック機構を設け、予め定められた順序でコマンドが送信されない場合はエラーとして処理することにより、不正な使用を防ぐことを目的とするものである。
【０００９】
【課題を解決するための手段】本発明は、命令入力部、応答出力部、命令解析部、命令処理実行部、データを記憶する不揮発性メモリを備えたＩＣカードにおいて、不揮発性メモリに命令の実行順序を登録したテーブルを備えたことを特徴とする。また本発明は、各命令が実行順序を示す番号を備えたことを特徴とする。また本発明は、認証が成立したことを条件に、前記テーブルに規定された実行順序を書き換えることができる専用の命令を有することを特徴とする。
【００１０】
【発明の実施の形態】以下、本発明の実施の形態について説明する。図１は本発明のＩＣＣを説明する図であり、図８と同一参照数字は同一内容を示している。図２は本発明において用いられるコマンドの構成を説明する図、図３は使用されるコマンドの例を説明する図、図４は実行順序テーブルを説明する図である。図１に示すＩＣＣは、メモリ１４内にコマンドの実行順序を規定する実行順序テーブル１４ａを備えた以外は図８で説明したものと同じであるので、その詳細な説明は省略する。本

発明においては、ＩＣＣのサポートするコマンドそれぞれがユニークなコマンド番号を持ち、その実行順序がコマンド番号を使ってテーブル１４ａに登録されており、登録された実行順序に合致するコマンドは適正に処理され、それに合致しないコマンドはエラーとなる。

【００１１】例えば、ＩＣＣが３つのコマンド、ＲＥＡＤ（読取り）コマンド、ＷＲＩＴＥ（書き込み）コマンド、ＥＲＡＳＥ（消去）コマンドをサポートしているとすると、図３に示すようにそれぞれにコマンド番号０１、０２、０３が割当られ、さらにＶＥＲＩＦＹ（認証）コマンドには０４を割り当てる。このコマンド番号を利用して実行順序テーブル１４ａには予めその順番が登録されている。コマンド番号はコマンドコード（ＩＮＳ）を利用するのがよい。

【００１２】図４（ａ）は実行順序テーブルの１例を示すもので、リッセト（活性化）直後のコマンドにのみ適用するのか否かのフラグがＯＮになっている場合を例に説明する。このフラグは、図４（ｂ）に示すように、００の場合はリセット直後のコマンドに適用、０１の場合はリセット直後のコマンド以外にも適用するものである。もちろんこのような規定をせず、常時コマンド順序が適用されるようにしてもよい。この例では、１コマンド目がコマンド番号０３、２コマンド目がコマンド番号０２となっている場合に正常処理が行われ、これ以外の順番ではエラとなる。すなわち、１コマンド目に記載されているコマンドを受信すると、次のコマンドは２番目に指定されているコマンド以外は受付なくなり、ＩＣＣからはエラーステータスが返される。こうして誤ったコマンドシーケンスによる利用を防止することができる。なお、番号を付して前後の順番を間違わないようにするコマンドは、特に重要なコマンドに対して行うようにしても良く、また番号を付すコマンドの数はテーブルの許す範囲で広げることができる。

【００１３】図５は実行順序指定によるコマンド処理の１例を示す処理フローであり、この処理では送信されるコマンド１つ１つについての処理を実行し、順番が間違った段階でエラーステータスを返すものである。ＩＣＣを活性化し、外部からＩＣＣへコマンドが送信されると、ＩＣＣではコマンド受信処理を行う（ステップＳ１～Ｓ３）。次いで、ＩＣＣでは図４（ｂ）に示したフラグのチェックを行い、フラグがセットされているか否かを判断する（ステップＳ４、Ｓ５）。フラグがセットされている場合は、リセット直後のコマンドにのみ適用されるため、リセット直後のコマンドか否かを判断し、リセット直後のコマンドであれば、テーブルチェックを行い、また、ステップＳ５でフラグがリセットされている場合はリセット直後以外のコマンドにも適用されるためテーブルチェックを行う（ステップＳ６、Ｓ７）。テーブルチェックを行ってコマンド実行順序が一致している場合、あるいはステップＳ６でリセット直後のコマンドでない場合は、そのままコマンド処理を実行し（ステップＳ９）、ＩＣＣから正常な処理が行われたことを接続装置へレスポンスとして返し（ステップＳ１０）、以上の処理が最後のコマンドまで実行される（ステップＳ１１）。また、ステップＳ８において、テーブルに登録した実行順序と不一致の場合には、その時点でレスポンス処理でエラーステータスを返し処理を終了する。

【００１４】前述したように、コマンドの実行順序は不揮発性メモリにテーブルとして登録されているが、この実行順序は専用のコマンドを用いてＩＣＣ発行処理後に変更するようにしてもよく、そうした例について以下に説明する。図６は実行順序テーブルを書き換える専用のコマンドの構成を示し、例えば命令コードが９９の場合はこの専用のコマンドとする。専用コマンドのデータ部の００は図４（ｂ）で示したフラグに相当し、このコマンドではリセット直後に適用することを示している。次の２バイトの０１、０２はコマンドの実行順序を示している。こうしてリセット直後に適用か否かのフラグと、コマンド実行順序が新たに書き換えられる。なお、このコマンドは認証処理が成功したときのみ行えることとし、正当な権利を持つ人以外は実行できないようにしておく必要がある。

【００１５】図７は実行順序テーブルを書き換える処理を説明する図である。ＩＣＣを活性化し、外部からＩＣＣへコマンドを送信し、ＩＣＣ側でコマンド受信処理を行う（ステップＳ４１～Ｓ４３）。次いで、認証処理を実行し（ステップＳ４４）、認証ＯＫか否か判断し（ステップＳ４５）、認証が成功しなかった場合には処理は終了する。認証が成功した場合には命令コードを見て、順序テーブル書換えコマンドか否か判断する（ステップＳ４６）。順序テーブル書き換えコマンドでない場合は処理は終了する。順序テーブル書き換えコマンドの場合には、リセット直後に適用するフラグをセットするのか否かを判断し（ステップＳ４７）、セットの場合にはフラグセット処理、セットでない場合はフラグリセット処理をそれぞれ行い（ステップＳ４８，４９）、次いで、順序テーブル書き換え処理を実行する（ステップＳ５０）。　こうして認証が成功した正当な権利を持つ人のみがフラグセット処理、実行順序テーブル書き換え処理を行うことができる。

【００１６】

【発明の効果】以上のように本発明によれば、ＩＣカード内にチェック機構を設け、ＩＣカード内の機能を利用する時には、予め定められた手順に従ってコマンドをＩＣカードへ送らなければ違反と見なしエラーステータスが返されるので、誤ったコマンドシーケンスの利用を防止し、偽造ＩＣカードや偽造端末による不正利用を防ぐことが可能となる。

【図面の簡単な説明】

【図１】　本発明のＩＣカードを説明する図である。

【図２】　本発明のコマンドの構成を説明する図である。

【図３】　本発明で使用されるコマンドの例を説明する図である。

【図４】　実行順序テーブルを説明する図である。

【図５】　順序指定によるコマンド処理の１例を示す処理フローを示す図である。

【図６】　実行順序テーブルを書き換える専用のコマンドの構成を示す図である。

【図７】　実行順序テーブルを書き換える処理を説明す＊る図である。

【図８】　従来のＩＣＣを説明する概略図である。

【図９】　キャラクタを説明する図である。

【図１０】　ブロックを説明する図である。

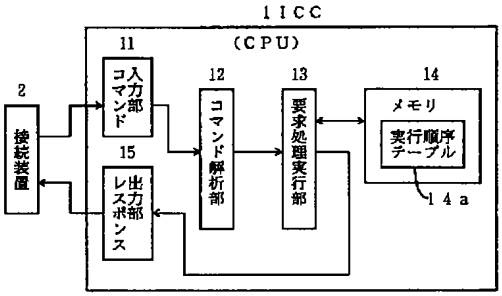
【図１１】　コマンドを説明する図である。

【図１２】　レスポンスを説明する図である。

【符号の説明】

１…ＩＣカード、２…接続装置、１２…コマンド解析部、１３…コマンド処理実行部、１４…メモリ、１４ａ…実行順序テーブル。

【図１】



【図２】

CLA	INS	P1	P2	Lc	cデータ	Le

【図１２】

← 本体部 →		← 後続部 →
rデータ	SW1	SW2

【図６】

CLA	INS	P1	P2	Lc	データ		
9 0	9 9	0 0	0 0	0 3	0 0	0 1	0 2

【図３】

コマンド番号	コマンド名
0 1	READコマンド
0 2	WRITEコマンド
0 3	ERASEコマンド
0 4	VERIFYコマンド

【図４】

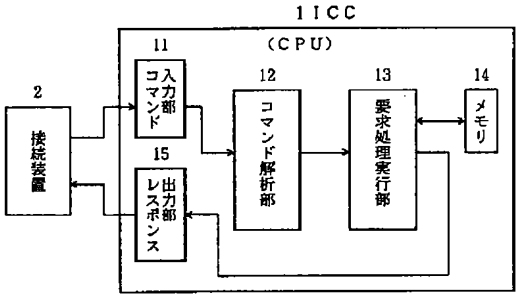
(a)

リセット直後のコマンドに適用	1コマンド目	2コマンド目
ON	0 3	0 2

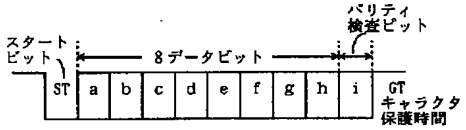
(b)

0 0	リセット直後のコマンドに適用
0 1	リセット直後のコマンド以外に適用

【図８】



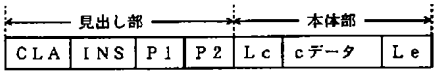
【図９】



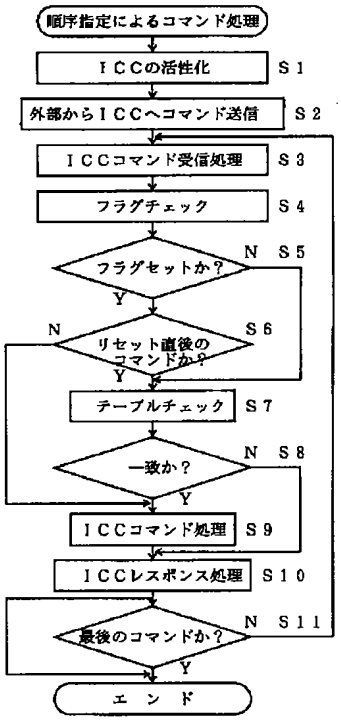
【図１０】

先頭フィールド			情報フィールド	最終フィールド
NAD 1バイト	PCB 1バイト	LEN 1バイト	INF 0～254バイト	EDC 1又は2バイト

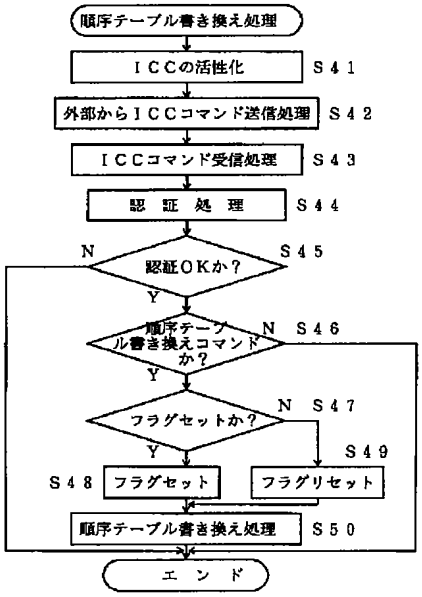
【図１１】



【図５】


順序指定によるコマンド処理
ＩＣＣの活性化
Ｓ１
外部からＩＣＣへコマンド送信
Ｓ２
ＩＣＣコマンド受信処理
Ｓ３
フラグチェック
Ｓ４
フラグセットか？
Ｎ
Ｓ５
Ｙ
リセット直後のコマンドか？
Ｎ
Ｓ６
Ｙ
テーブルチェック
Ｓ７
一致か？
Ｎ
Ｓ８
Ｙ
ＩＣＣコマンド処理
Ｓ９
ＩＣＣレスポンス処理
Ｓ１０
最後のコマンドか？
Ｎ
Ｓ１１
Ｙ
エ　ン　ド

【図７】


順序テーブル書き換え処理
ＩＣＣの活性化
Ｓ４１
外部からＩＣＣコマンド送信処理
Ｓ４２
ＩＣＣコマンド受信処理
Ｓ４３
認　証　処　理
Ｓ４４
Ｎ
認証ＯＫか？
Ｓ４５
Ｙ
順序テーブル書き換えコマンドか？
Ｎ
Ｓ４６
Ｙ
フラグセットか？
Ｎ
Ｓ４７
Ｙ
Ｓ４８
フラグセット
フラグリセット
Ｓ４９
順序テーブル書き換え処理
Ｓ５０
エ　ン　ド